#2

PATENT
81942.0009
Express Mail Label No. EL 713 695 994 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Yasuyuki MURAKAMI	Examiner: Not assigned
Serial No: Not assigned	
Filed: January 22, 2001	
For: COMMON KEY GENERATING METHOD, COMMON KEY GENERATING APPARATUS, ENCRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM	

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016359 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 22, 2001

By: _____
Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

#2

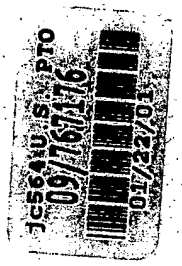
日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

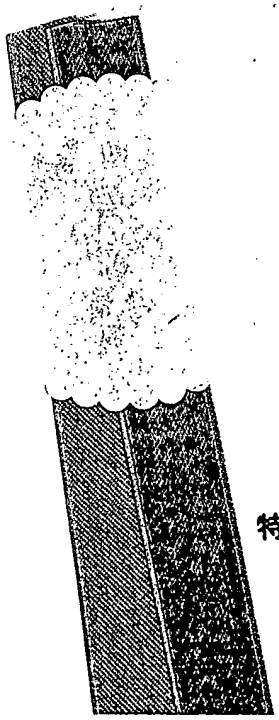
出願年月日
Date of Application: ２０００年 １月２５日

出願番号
Application Number: 特願２０００－０１６３５９

出願人
Applicant (s): 村田機械株式会社
笠原 正雄



CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年 ８月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６４８４

【書類名】　特許願

【整理番号】　20876

【提出日】　平成12年 1月25日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04L 9/00

【発明の名称】　共通鍵生成方法，共通鍵生成装置及び暗号通信方法

【請求項の数】　3

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　共通鍵生成方法，共通鍵生成装置及び暗号通信方法

【特許請求の範囲】

【請求項１】　エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、一方のエンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成することを特徴とする共通鍵生成方法。

【請求項２】　暗号通信システムのエンティティに設けられており、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する装置において、前記エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記エンティティ固有の各秘密鍵に含まれている通信相手のエンティティに対応する成分を夫々選び出す手段と、選び出した成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成する手段とを備えることを特徴とする共通鍵生成装置。

【請求項３】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の複数の秘密鍵に含まれている相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記相手のエンティティに対応する夫々の成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成すること

を特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、平文を暗号文に変換する暗号化処理及び暗号文を平文に変換する復号処理に用いる共通鍵を生成する方法及び装置、並びに、生成した共通鍵を利用して暗号通信を行う暗号通信方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が

等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【０００５】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した３つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系としてＲＳＡ暗号系が提案された。このＲＳＡ暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【０００６】

また、各エンティティの住所，氏名等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案された。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、このＩＤ情報に基づく暗号技法には、（１）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（２）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（２）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中枢をなすものと考えられている。

【０００７】

この（２）の手法による暗号系は、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。ＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者に

よるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【０００８】

図６は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図６において、エンティティＸの特定情報であるエンティティＸの名前，住所，電話番号等のＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ID_X）で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝，センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報ｈ（ID_X）に基づいて、以下のように秘密情報S_{Xi}を計算し、秘密裏にエンティティＸへ配布する。

$$S_{Xi}=F_i\ (\{SC_i\},\ \{PC_i\},\ h(ID_X))$$

【０００９】

エンティティＸは他の任意のエンティティＹとの間で、暗号化，復号のための共通鍵K_{XY}を、エンティティＸ自身の秘密情報｛S_{Xi}｝，センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報ｈ（ID_Y）を用いて以下のように生成する。

$$K_{XY}=f\ (\{S_{Xi}\},\ \{PC_i\},\ h(ID_Y))$$

また、エンティティＹも同様にエンティティＸへの鍵を共通鍵K_{YX}を生成する。もし常に$K_{XY}=K_{YX}$の関係が成立すれば、この鍵K_{XY}，K_{YX}をエンティティＸ，Ｙ間で暗号化鍵，復号鍵として使用できる。

【００１０】

上述した公開鍵暗号系では、例えばＲＳＡ暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ＩＤ－ＮＩＫＳでは、各ＩＤ情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図６に示すようなＩＤ－ＮＩＫＳのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ＩＤ－ＮＩＫＳが将来の暗号系の中心になると期待されている。

【００１１】

このＩＤ－ＮＩＫＳには、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【００１２】

この結託問題の難しさは、特定情報（ＩＤ情報）に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。ＩＤ－ＮＩＫＳでは、センタの公開パラメータと個人の公開された特定情報（ＩＤ情報）とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【００１３】

そこで、本発明者等は、特定情報（ＩＤ情報）をいくつかに分割し、複数のセンタの夫々からその分割した特定情報（ＩＤ情報）に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる秘密鍵生成方法，暗号化方法及び暗号通信方法（以下、これらを先行例という）を提案している。

【００１４】

結託問題を解決することを目的として提案されてきたエンティティの特定情報（ＩＤ情報）に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報（ＩＤ情報）をいくつかに分割し、分割した各特定情報（ＩＤ情報）についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【００１５】

先行例では、信頼される複数のセンタが設けられ、各センタは各エンティティの分割した各特定情報（ＩＤ情報）に対応する数学的構造を持たない秘密鍵を夫々生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ＩＤ情報）とから共通鍵を、予備通信を行わずに生成する。これらの各秘密鍵に含まれている、通信相手に対応する成分を夫々取り出し、取り出した成分を合成加算して共通鍵を生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【００１６】

【発明が解決しようとする課題】

そして、本発明者等は、このような先行例の改良を研究しており、その先行例を適用した暗号通信システムの構築を図っている。このような複数のセンタを設けた暗号通信システムにとっては、予備通信を行うことなく暗号化処理及び復号処理に使用する共通鍵を生成できて、便利である。ところが、各秘密鍵に含まれている通信相手に対応する成分を単純に合成加算する場合には、各成分のビット数が固定であるので、得られる共通鍵のビット数も固定となり、任意のビット数の鍵共有システムに適応できないという難点があり、更なる改善が望まれている。

【００１７】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティが生成する共通鍵を可変長にできて、任意のビット数の鍵共有システムに適応できる共通鍵生成方法，共通鍵生成装置及び暗号通信方法を提供することを目的とする。

【００１８】

【課題を解決するための手段】

請求項１に係る共通鍵生成方法は、エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、一方のエンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記一方のエンティティ固有の各秘密鍵に

含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成することを特徴とする。

【００１９】

請求項２に係る共通鍵生成装置は、暗号通信システムのエンティティに設けられており、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する装置において、前記エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記エンティティ固有の各秘密鍵に含まれている通信相手のエンティティに対応する成分を夫々選び出す手段と、選び出した成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成する手段とを備えることを特徴とする。

【００２０】

請求項３に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の複数の秘密鍵に含まれている相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記相手のエンティティに対応する夫々の成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成することを特徴とする。

【００２１】

本発明では、一方のエンティティの各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分に対してビットを拡大する変換を施したものを合成して共通鍵を生成する。よって、取り出した成

分と異なるビット数の共通鍵を生成できる。このようなビット数変換の合成処理として、例えば、ずらし合成処理を利用できる。取り出した各成分がｎビットである場合に、それらを単純に合成したときにはその合成結果はｎビットとなり、共通鍵の大きさは固定化（ｎビット）する。そこで、本発明では、これらの各ｎビットの複数の成分をずらせて合成する。このようなずらし合成を行うことによって、その合成結果はｍビット（ｍ＞ｎ）となり、ｍビットの共通鍵を生成できる。また、そのずらし量を調整することにより任意の大きさの共通鍵を生成できる。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｊ個）のセンタ１が設定されており、これらのセンタ１としては、例えば社会の公的機関を該当できる。

【００２３】

これらの各センタ１と、この暗号通信システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは、通信路2_{a1}，…，2_{aJ}、2_{b1}，…，2_{bJ}、・・・、2_{z1}，…，2_{zJ}により接続されており、これらの通信路を介して、各センタ１から各エンティティ固有の秘密鍵が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００２４】

図２は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図２の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ送信し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００２５】

ｊ（ｊ＝１，２，・・・，Ｊ）番目のセンタ１には、各エンティティのａ，ｂの分割特定情報（分割ＩＤベクトル）を用いて各エンティティａ，ｂ固有の秘密鍵を生成する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵がエンティティａ，ｂへ送付される。

【００２６】

エンティティａ側には、Ｊ個の各センタ１から送られる固有の秘密鍵をテーブル形式で格納しているメモリ１０と、これらの秘密鍵の中からエンティティｂに対応する成分を選び出す成分選出器１１と、選び出されたこれらの成分を合成してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００２７】

また、エンティティｂ側には、各センタ１から送られる固有の秘密鍵をテーブル形式で格納しているメモリ２０と、これらの秘密鍵の中からエンティティａに対応する成分を選び出す成分選出器２１と、選び出されたこれらの成分を合成してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路３０から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００２８】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

【００２９】

（予備処理）

各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図３に示すようにそのＩＤベクトルをブロックサイズM_1，M_2，・・・，M_J毎にＪ個のブロックに分割する。例えば、エンティティａのＩＤベクトル（ベクトルI_a）を下記（１）のように分割する。分割特定情報である各ベクトルI_{aj}（ｊ＝１，２，・・・，Ｊ）をＩＤ分割ベクトルと呼ぶ。こ

こで、M_j ＝Ｍとすると、全てのＩＤ分割ベクトルのサイズが等しくなる。また、M_j ＝１と設定することも可能である。なお、各エンティティの公開ＩＤベクトルはハッシュ関数により、Ｌビットに変換される。

【００３０】

【数１】

$$\overrightarrow{I_a} = [\overrightarrow{I_{a1}} | \overrightarrow{I_{a2}} | \cdots | \overrightarrow{I_{aJ}}] \quad \cdots (1)$$

【００３１】

（秘密鍵の生成処理（エンティティの登録処理））

エンティティａに登録を依頼された各センタ１は、秘密鍵発行器１ａにて、エンティティａのＩＤ分割ベクトルとセンタ１自身の秘密情報（後述する対称行列）とを用いて、エンティティａ固有の秘密鍵（後述する秘密鍵ベクトル）を生成し、生成した秘密鍵をエンティティａへ送信して、登録を完了する。

【００３２】

ここで、各センタ１での秘密情報（対称行列）、及び、各エンティティ固有の秘密鍵（秘密鍵ベクトル）の具体的内容について説明する。ｊ（ｊ＝１，２，・・・，Ｊ）番目のセンタ１は、秘密情報として、ランダムな数を要素とする対称行列H_j （$2^{Mj} \times 2^{Mj}$）を有している。そして、各エンティティに対して、対称行列H_j のそのエンティティの分割ＩＤベクトルに対応する行ベクトルを秘密鍵（秘密鍵ベクトル）として発行する。即ち、エンティティａに対しては、H_j 〔ベクトルI_{aj}〕を発行する。このH_j 〔ベクトルI_{aj}〕は、対称行列H_j よりベクトルI_{aj}に対応した行を１行抜き出したベクトルを表す。

【００３３】

（エンティティ間の共通鍵の生成処理）

エンティティａ（エンティティｂ）は、成分選出器１１（２１）にて、Ｊ個の各センタ１から送られた自身固有の秘密ベクトル（秘密鍵）をメモリ１０（２０）から読み出し、読み出した秘密ベクトル（秘密鍵）に含まれているエンティティｂ（エンティティａ）に対応する成分を取り出し、共通鍵生成器１２（２２）にて、これらＪ個の成分を合成して、エンティティａ（エンティティｂ）のエン

ティティｂ（エンティティａ）に対する共通鍵K_{ab}（K_{ba}）を生成する。ここで、Ｊ個の各センタ１が有する秘密情報（行列）の対称性に基づいて、両共通鍵K_{ab}，K_{ba}は一致する。

【００３４】

（エンティティａでの暗号文作成，エンティティｂでの暗号文復号）

エンティティａにおいて、共通鍵生成器１２で生成された共通鍵K_{ab}を用いて、暗号化器１３にて、平文（メッセージ）Ｍが暗号文Ｃに暗号化されて、その暗号文Ｃが通信路３０を介してエンティティｂへ伝送される。エンティティｂにおいて、共通鍵生成器２２で生成された共通鍵K_{ba}を用いて、復号器２３にて、暗号文Ｃが元の平文（メッセージ）Ｍに復号される。

【００３５】

ここで、本発明の特徴部分である各エンティティでの共通鍵の生成、特に、自身の秘密鍵に含まれる通信相手のエンティティに対応する成分の合成について説明する。

【００３６】

各エンティティにとって、共通鍵の生成における成分合成の仕方は任意であるので、各エンティティが、既に取得している自身の秘密鍵に含まれる通信相手のエンティティに対応する成分に対してその大きさを大きくする（ビットを拡大する）変換を行った後に、それらの成分を合成すれば、生成する共通鍵の大きさを大きくできる。即ち、ｊ番目の各センタ１はＳビットをＳ′ビットにに変換する関数F_jを公開し、エンティティａが、下記（２）に従ってエンティティｂに対する共通鍵K_{ab}を生成すれば良い。なお、$k_{ajbj}^{(j)}$は、エンティティａの秘密ベクトル（秘密鍵）に含まれているエンティティｂに対応する成分を示す。

【００３７】

【数２】

$$K_{ab}=F_1(k_{a_1b_1}^{(1)})\oplus F_2(k_{a_2b_2}^{(2)})\oplus\cdots\oplus F_J(k_{a_Jb_J}^{(J)}) \quad \cdots(2)$$

【００３８】

このような共通鍵を大きくする変換方法については、種々の方式が可能であるが、複雑な数学的構造を有さない点に信頼性を置く本発明の特徴を損なわないためには、ずらし合成（ビットローテション）などを利用した単純な変換が望ましいと考えられる。例えば、６４ビットの各成分から１２８ビットの共通鍵を生成するためには、≪ｎを１２８ビットレジスタに対するｎビットの左ローテション操作（上位にあふれた分は下位に戻る）として、下記（３）に従って共通鍵K_{ab}を生成すれば良い。

【００３９】

【数３】

$$K_{ab} = k^{(1)}_{a_1 b_1} \oplus (k^{(2)}_{a_2 b_2} \ll 32) \oplus (k^{(1)}_{a_1 b_1} \ll 64) \oplus (k^{(2)}_{a_2 b_2} \ll 96) \quad \cdots (3)$$

【００４０】

このようなずらし合成処理の具体例について説明する。以下の例では、合成すべき各成分のビット数は６４ビットであり、また、センタ１の設置個数を４個（Ｊ＝４）とする。６４ビットである４個の各成分を単純に加算合成した場合には、図４（ａ）に示すように、その合成結果は６４ビットとなる。よって、６４ビットの鍵共有システムについては適合できるが、他のビット数の鍵共有システムに適合できない。そこで、本発明では、図４（ｂ）に示すように、６４ビットである４個の各成分をずらせて加算合成する。例えば、図４（ｂ）の例では、その合成結果が１２８ビットとなるようにずらせていて、１２８ビットの共通鍵を生成できており、各成分が６４ビットであっても１２８ビットの鍵共有システムに適合できる。

【００４１】

なお、各成分のずらし量は任意に設定できるので、適合すべき鍵共有システムのビット数に応じて、そのずらし量を設定すれば良い。よって、このようなずら

し合成処理を行うことにより任意の大きさの共有鍵を生成でき、任意のビット数の鍵共有システムに適合できる。また、このずらし加算合成処理において、各位において乱数が消去されるようにずらし位置を設定するようにした場合には、乱数を付加した暗号化方式にも本発明を適用できる。

【００４２】

図５は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各エンティティにおいて自身固有の秘密鍵に含まれている、通信相手のエンティティに対応する成分を取り出す処理と、取り出した成分をずらし合成して、暗号化及び復号に用いる共通鍵を生成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各エンティティ側に設けられている。

【００４３】

図５において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各エンティティにおいて共通鍵を生成する。

【００４４】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各エンティティにおいて共通鍵を生成する。

【００４５】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピ

ュータ４０を制御することにより、各エンティティにおいて共通鍵を生成する。

【００４６】

【発明の効果】

以上のように、本発明では、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する際に、一方のエンティティの各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をずらし合成するようにしたので、任意の大きさの共通鍵を生成でき、任意のビット数の鍵共有システムに適合することが可能である。よって、ＩＤ－ＮＩＫＳ方式の暗号通信システムの発展に大いに寄与できる。

【００４７】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）請求項１に記載の共通鍵生成方法であって、取り出した成分に対してビットを拡大する変換を施したものを合成する際に、ずらし合成を利用する共通鍵生成方法。

（２）請求項２に記載の共通鍵生成装置であって、夫々の成分に対してビットを拡大する変換を施したものを合成し選び出した成分に対してビットを拡大する変換を施したものを合成する際に、ずらし合成を利用するようにした共通鍵生成装置。

（３）請求項３に記載の暗号通信方法であって、夫々の成分に対してビットを拡大する変換を施したものを合成する際に、ずらし合成を利用する暗号通信方法。

（４）　各エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている暗号文の送信先の相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、前記相手のエンティティに対応する夫々の成分に対してビットを拡大する変換を施したものを合成して、暗号化に用いる前記共通鍵を生成する暗号化方法。

（５）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互

に行うこととし、各エンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身固有の複数の秘密鍵に含まれている、通信対象のエンティティに対応する成分を使用して、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、前記通信対象のエンティティに対応する夫々の成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成するようにした暗号通信システム。

（６）　コンピュータに、エンティティ間の暗号通信における、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、一方のエンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出すことをコンピュータに実行させるプログラムコード手段と、取り出した成分に対してビットを拡大する変換を施したものを合成して前記共通鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図３】

エンティティのＩＤベクトルの分割例を示す模式図である。

【図４】

従来例と本発明例とにおける、エンティティ自身の秘密鍵に含まれる通信相手のエンティティに対応する成分の合成処理を示す模式図である。

【図５】

記録媒体の実施の形態の構成を示す図である。

【図６】

ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１　センタ

１ａ　秘密鍵生成器

１０，２０　メモリ

１１，２１　成分選出器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

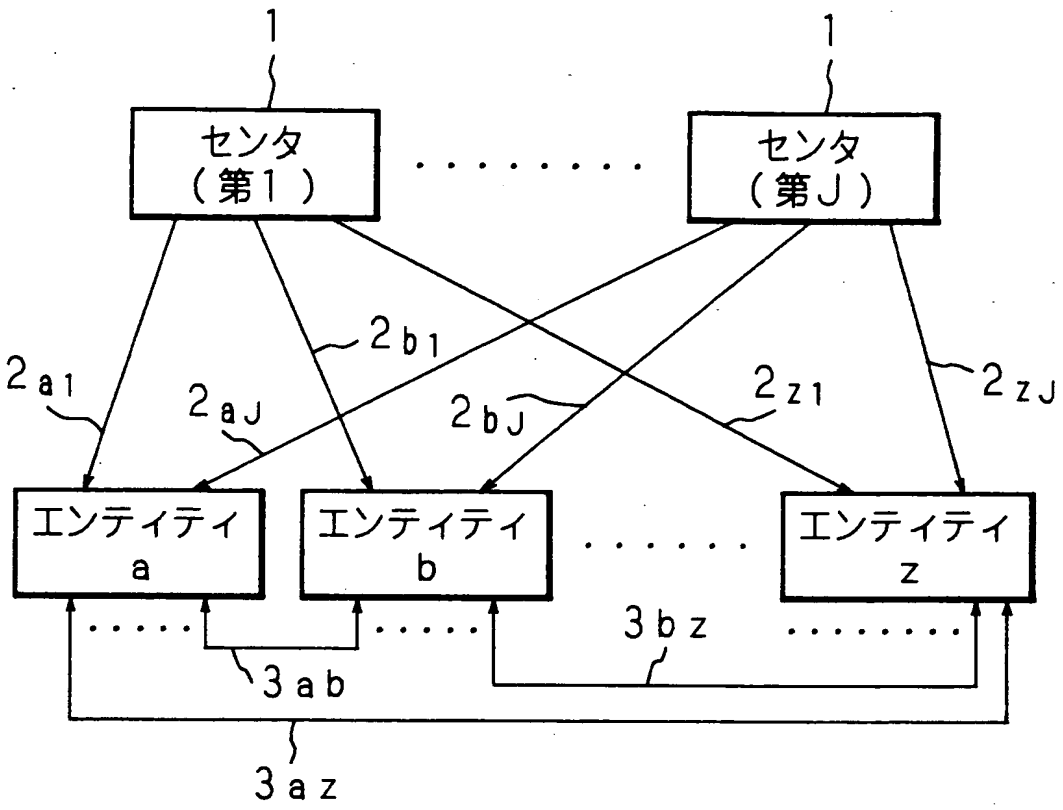
３０　通信路

４０　コンピュータ

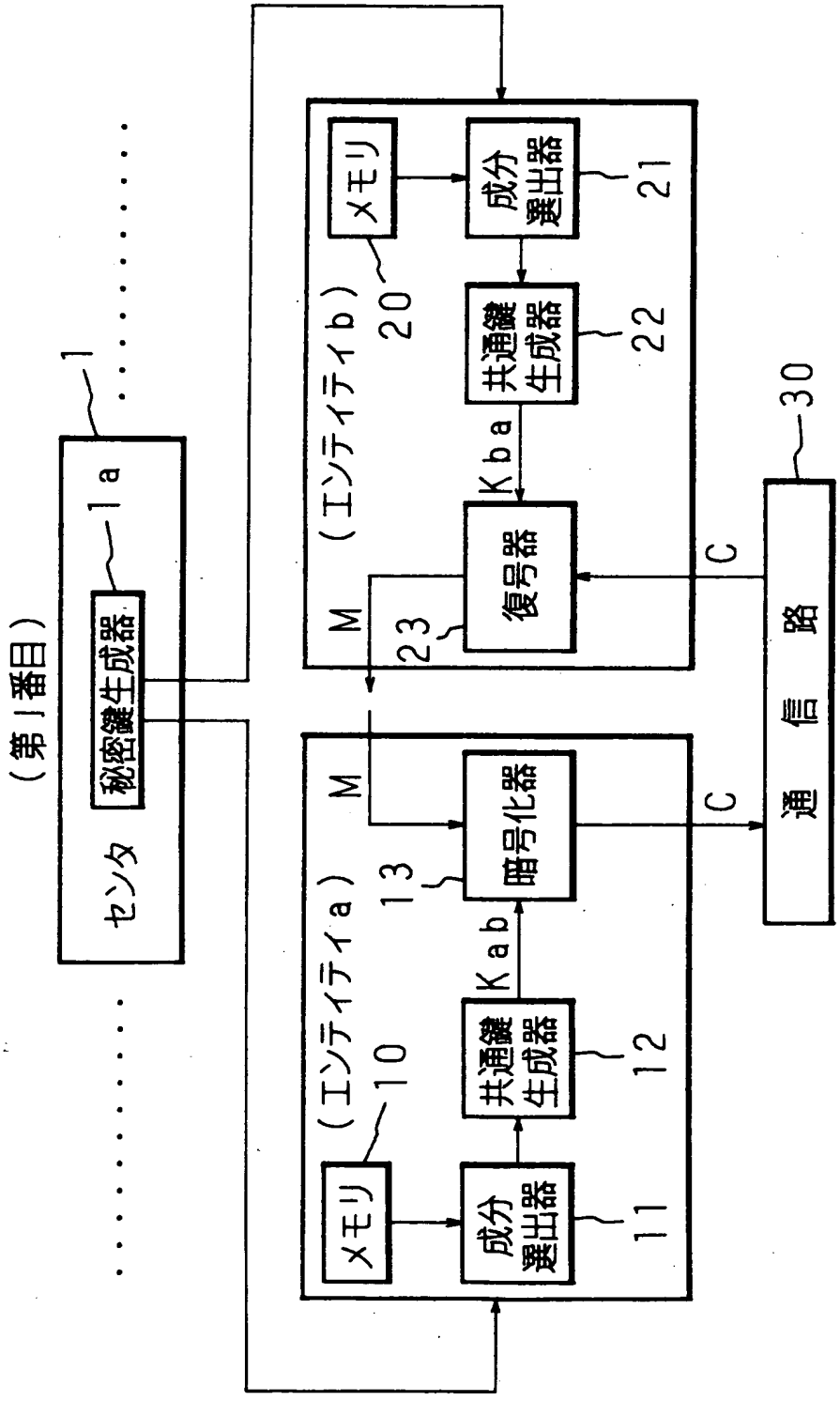
４１，４２，４３　記録媒体

【書類名】　　図面

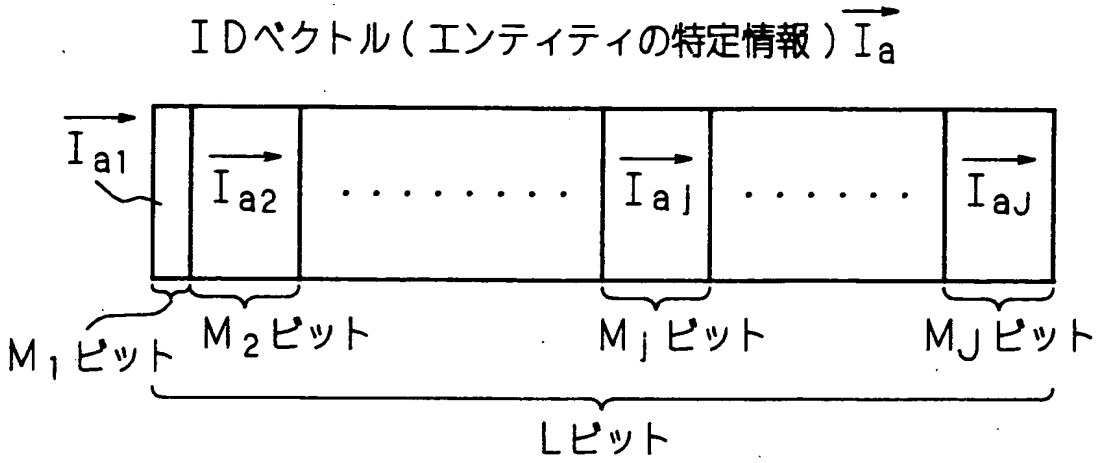
【図１】


1
1
センタ
（第1）
センタ
（第J）
2a1
2aJ
2b1
2bJ
2z1
2zJ
エンティティ
a
エンティティ
b
エンティティ
z
3ab
3bz
3az

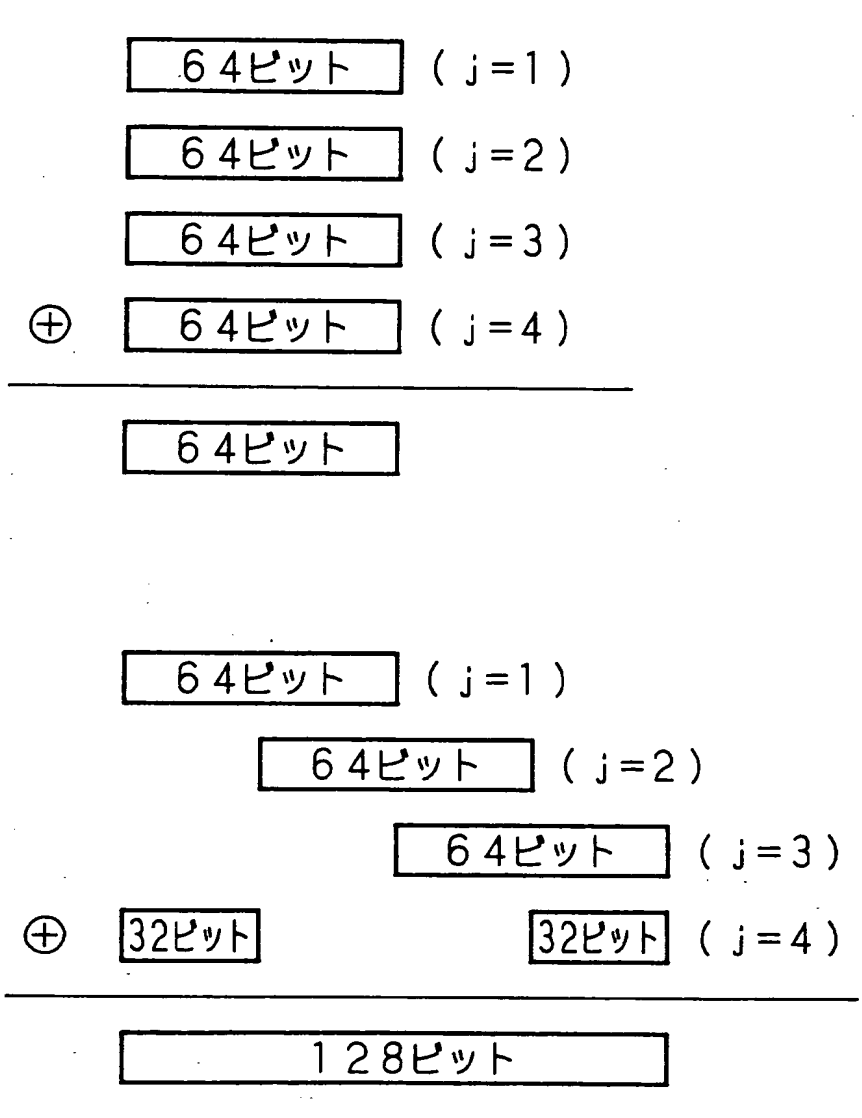
【図２】


（第ｉ番目）
センタ
秘密鍵生成器
1a
1
（エンティティｂ）
20
メモリ
成分選出器
21
共通鍵生成器
22
Kba
復号器
23
M
C
30
通信路
（エンティティａ）
10
メモリ
成分選出器
11
共通鍵生成器
12
Kab
暗号化器
13
M
C

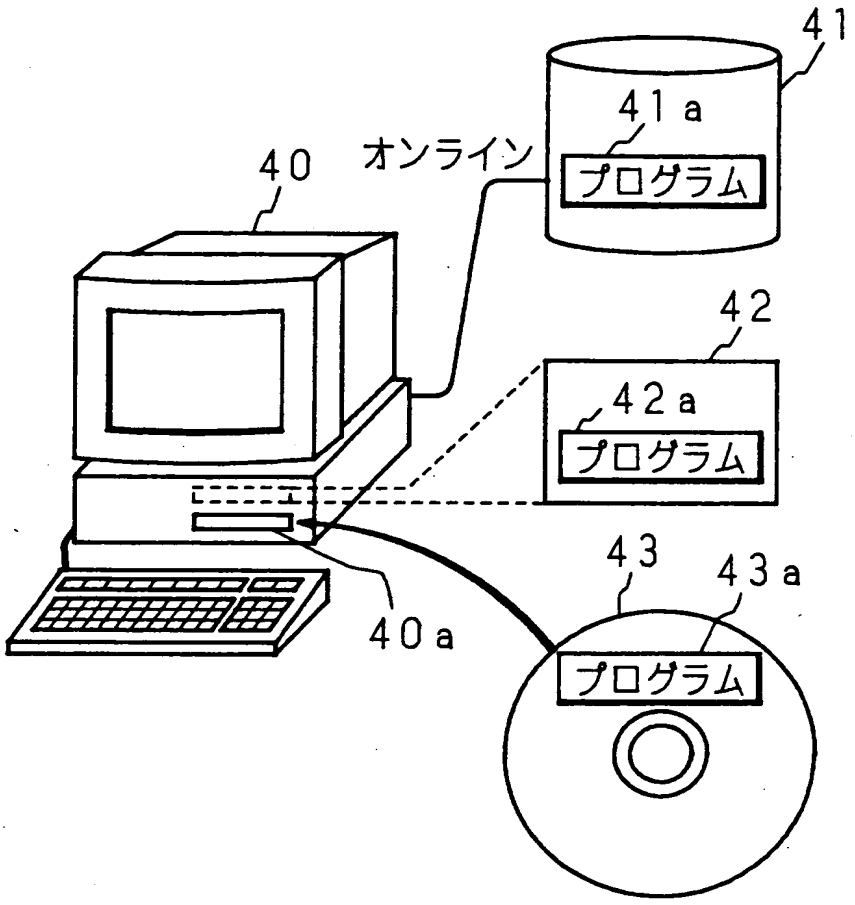
【図３】


ＩＤベクトル（エンティティの特定情報）$\vec{I_a}$
$\vec{I_{a1}}$
$\vec{I_{a2}}$
$\vec{I_{aj}}$
$\vec{I_{aJ}}$
M_1ビット
M_2ビット
M_jビット
M_Jビット
Lビット

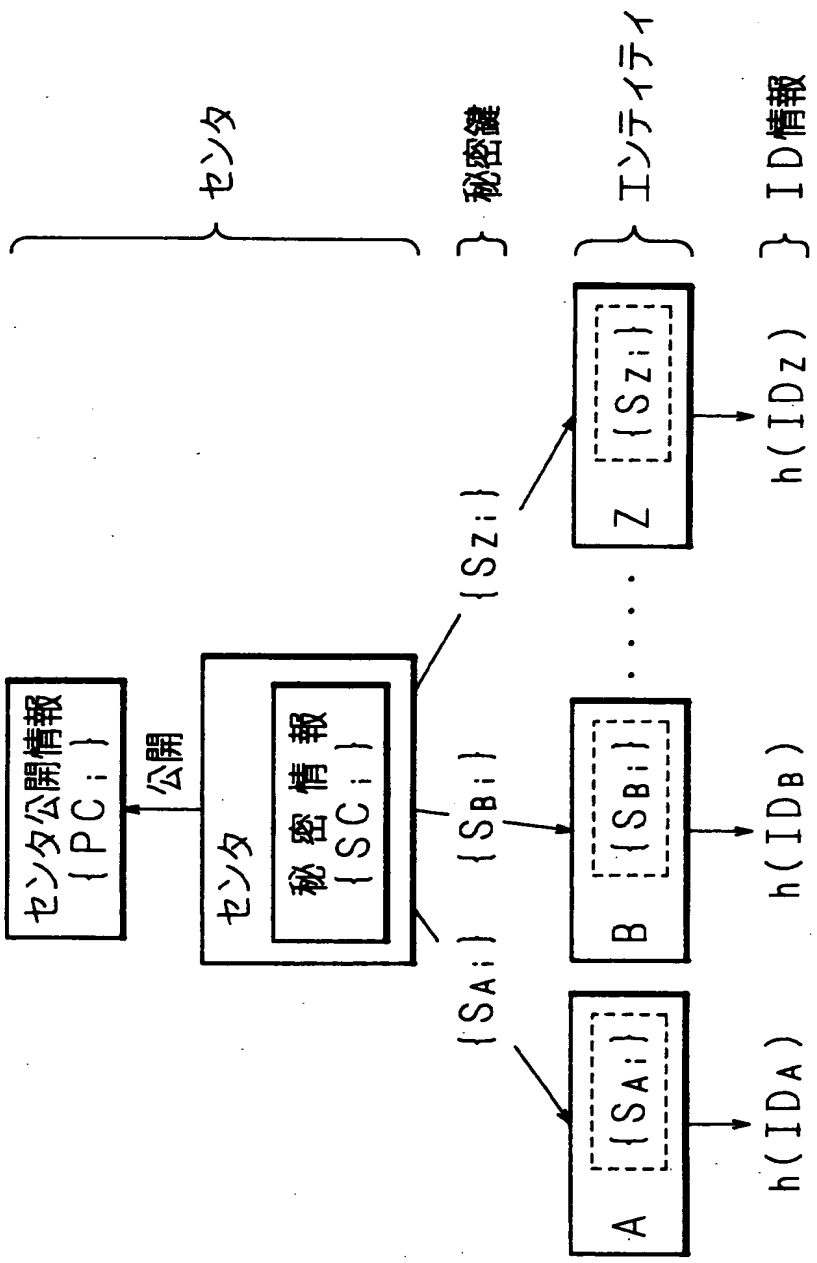
【図４】


（ａ）
６４ビット
（ｊ＝１）
６４ビット
（ｊ＝２）
６４ビット
（ｊ＝３）
⊕
６４ビット
（ｊ＝４）
６４ビット
（ｂ）
６４ビット
（ｊ＝１）
６４ビット
（ｊ＝２）
６４ビット
（ｊ＝３）
⊕
32ビット
32ビット
（ｊ＝４）
１２８ビット

【図５】



【図６】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SZi}
{SBi}
{SAi}
Z
{SZi}
h(IDz)
B
{SBi}
h(IDB)
A
{SAi}
h(IDA)

【書類名】　　要約書

【要約】

【課題】　各エンティティが生成する共通鍵を可変長にできて、任意のビット数の鍵共有システムに適応できる共通鍵生成方法，共通鍵生成装置及び暗号通信方法を提供する。

【解決手段】　平文Ｍから暗号文Ｃへの暗号化処理及び暗号文Ｃから平文Ｍへの復号処理に用いる共通鍵を生成する際に、成分選出器１１（２１）にて、一方のエンティティａ（ｂ）の各秘密鍵に含まれている、通信相手である他方のエンティティｂ（ａ）に対応する成分を夫々取り出し、共通鍵生成器１２（２２）にて、取り出した成分をずらし合成して共通鍵K_{ab}（K_{ba}）を生成する。

【選択図】　　図３

認定・付加情報

特許出願の番号	特願２０００－０１６３５９
受付番号	５０００００７３７３８
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１２年　５月３０日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000006297

【住所又は居所】　京都府京都市南区吉祥院南落合町３番地

【氏名又は名称】　村田機械株式会社

【特許出願人】

【識別番号】　597008636

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名又は名称】　笠原　正雄

【復代理人】

【識別番号】　100114557

【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所

【氏名又は名称】　河野　英仁

【代理人】　申請人

【識別番号】　100078868

【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所

【氏名又は名称】　河野　登夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄